



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/026,848	12/21/2001	Ynjiun P. Wang	Wang P007	1158

7590 06/16/2004
MOSER, PATTERSON & SHERIDAN, LLP
350 CAMBRIDGE AVENUE, SUITE 250
Palo Alto,, CA 94306

EXAMINER

CHEUNG, MARY DA ZHI WANG

ART UNIT	PAPER NUMBER
----------	--------------

3621

DATE MAILED: 06/16/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/026,848

Applicant(s)

WANG, YNJIUN P.

Examiner

Mary Cheung

Art Unit

3621

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 05 April 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-17 is/are pending in the application.
- 4a) Of the above claim(s) 1-4 and 9 is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 5-8 and 10-17 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Status of the Claims

1. This action is in response to the Restriction Election filed on April 5, 2004. Claims 1-17 are pending. Claims 5-8 and 10-17 are elected. Claims 1-4 and 9 are withdrawn from consideration.

Claim Objections

2. Claims 5 and 13 are objected to because of the following informalities:

- a) In line 4 of claim 5, the apostrophe symbol after the word "key" should be deleted;
- b) In line 6 of claim 5, the phrase "the receiver's ID" should be --the receiver's user ID--;
- c) In line 6 of claim 5, the phrase "the user's ID" should be --the sender's user ID--;
- d) In line 2 of claim 13, the word "shares" should be --shared--.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 5-8 and 10-17 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 5 recites the limitation "the receiver's user ID" in line 3. There is insufficient antecedent basis for this limitation in the claim.

Claim 5 recites the limitation "the sender" in line 5. There is insufficient antecedent basis for this limitation in the claim.

Claim 5 recites the limitation "the receiving PEAD user" in line 7. There is insufficient antecedent basis for this limitation in the claim.

Claim 12 recites the limitation "the PEAD" in lines 1-2. It is not clear which PEAD it refers to.

Claim 13 recites the limitation "the PEAD" in line 2. It is not clear which PEAD it refers to.

Claims 6-8 and 10-17 are rejected for incorporating the errors of their respective base claim 5 by dependency.

Claim Rejections - 35 USC § 101

5. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

6. Claims 5-6 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

The basis of this rejection is set forth in a two-prong test of:

- (1) whether the invention is within the technological arts; and
- (2) whether the invention produces a useful, concrete, and tangible result.

For a claimed invention to be statutory, the claimed invention must be within the technological arts. Mere ideas in the abstract (i.e., abstract idea, law of nature, natural

Art Unit: 3621

phenomena) that do not apply, involve, use, or advance the technological arts fail to promote the "progress of science and the useful arts" (i.e., the physical sciences as opposed to social sciences, for example) and therefore are found to be non-statutory subject matter. For a process claim to pass muster, the recited process must somehow apply, involve, use, or advance the technological arts. In the present case, claims 5-6 only recite an abstract idea. The recited steps of merely exchanging messages between receivers and senders does not apply, involve, use, or advance the technological arts since all of the recited steps can be performed in the mind of the user or by use of a pencil and paper. These steps only constitute an idea of how to securely exchange messages over another.

As to technological arts recited in the preamble, mere recitation in the preamble (i.e., intended or field of use) or mere implication of employing a machine or article of manufacture to perform some or all of the recited steps does not confer statutory subject matter to an otherwise abstract idea unless there is positive recitation in the claim as a whole to breathe life and meaning into the preamble. In the present case, none of the recited steps are directed to anything in the technological arts as explained above with the exception of the recitation in the preamble that the method involve internet and server. Looking at the claim as a whole, nothing the body of the claim recites any structure or functionality to suggest that a computer performs the recited steps. Therefore, the preamble is taken to merely recite a field of use.

Additionally, for a claimed invention to be statutory, the claimed invention must produce a useful, concrete, and tangible result. In the present case, the claimed invention exchange messages (i.e., useful, concrete and tangible).

Although the recited process produces a useful, concrete, and tangible result, since the claimed invention, as a whole, is not within the technological arts as explained above, claim 5-6 are deemed to be directed to non-statutory subject matter.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

8. Claims 5-8 and 10-11 are rejected under 35 U.S.C. 102(e) as being anticipated by Dorenbos, U. S. Patent 5,751,813.

As to claim 5, Dorenbos teaches a method of exchanging secured messages between first and second registered PEAD users over the internet and a server comprising the steps of (column 3 line 1 – column 4 line 3 and Fig. 1; *specifically, the PEAD corresponds to items 103, 111, 115, 119, 121, 127 and 131 of Fig. 1*):

a) obtaining public key information using the receiver's user ID as an index (column 4 lines 23-25, 53-60);

- b) deriving a shared secret using the receiver's public key (column 3 lines 12-15; *specifically, the shared secret corresponds to the appended message that is derived from the first-stage encrypted message in Dorenbos' teaching*);
- c) the sender then encrypting a message with the shared secret and sending it with the receiver's ID appended with the user's ID (column 3 lines 34-36);
- d) then the receiving PEAD user using the sender's user ID and sender's public key information to derive the shared secret (column 4 lines 4-10).

As to claim 6, Dorenbos teaches storing one or more of the other PEAD users' share secret using the sender's ID as an index (column 4 lines 23-25).

As to claim 7, Dorenbos teaches the sender retrieves the public key information using the receiver's user ID from the server (column 4 lines 53-60).

As to claim 8, Dorenbos teaches after the sender encrypts the message with the shared secret, sending it to the server with the receiver's ID appended (column 3 lines 12-25 and Fig. 2).

As to claims 10-11, forwarding the message when the receiver's PEAD is polling for messages, and the server pushing the message to the receiver's PEAD are taught by Dorenbos as transmitting the message to the receiver's PEAD (column 3 lines 36-48).

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

10. Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Dorenbos, U. S. Patent 5,751,813 in view of Spies et al., U. S. Patent 6,055,314.

As to claim 12, Dorenbos teaches the sender's public key is stored on a server and is indexed by the sender's ID (column 4 lines 23-25). Dorenbos does not specifically teach the sender causing the PEAD to download a key pair comprising a public key and a private key, and then transferring the public key to a server. However, Spies teaches sender causing a portable electronic device to download cryptographic keys, and then transferring the keys to a server (column 6 lines 56 – column 7 lines 3 and column 7 lines 55-67 and Fig. 2). It would have been obvious to one of ordinary skill in the art at the time the invention was made to allow the teaching of Dorenbos to include the feature of having the PEAD download a key pair and then transferring the public key to a server so that the PEAD would be able to easily and quickly obtain the cryptographic keys for using them to securely transmitting messages.

Allowable Subject Matter

11. Claims 13-17 would be allowable if rewritten to overcome the rejection(s) under 35 U.S.C. 112, second paragraph, set forth in this Office action and to include all of the limitations of the base claim and any intervening claims.

Conclusion

12. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Blakley, III et al. (U. S. Patent 5,677,952) discloses a secret key is derived from a password entered into the computer by an authorized user.

Gennaro et al. (U. S. Patent 5,937,066) discloses two-phrases cryptographic key recovery system.

Liao et al. (U. S. Patent 6,263,437) discloses conducting crypto-ignition process between thin client devices and server devices.

Kato (U. S. Patent 6,381,331) discloses an information sending system for sending encrypted information which can be decrypted in units of parts of information.

Friedman et al. (WO 99/49613) discloses a key recovery authority exchanges static public keys with each of the nodes.

Inquire

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mary Cheung whose telephone number is (703)-305-0084. The examiner can normally be reached on Monday – Thursday from 8:00 AM to 5:30 PM. The examiner can also be reached on alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Trammell, can be reached on (703) 305-9768.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-308-1113.

The fax phone number for the organization where this application or proceedings is assigned are as follows:

(703) 872-9306 (Official Communications; including After Final
Communications labeled "BOX AF")
(703) 746-5619 (Draft Communications)

Hand delivered responses should be brought to Crystal Park 5, 2451 Crystal Drive, 7th Floor Receptionist.

Mary Cheung
Patent Examiner
Art Unit 3621
June 9, 2004



JAMES P. TRAMMELL
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600